

- 3/1 c1
At
end
- (d) receiving by the host computer the stored aggregated data from the client computer; and
(e) servicing by the host computer the received request based on the received, stored aggregated data to generate a request result.

Please delete claim 9 and 11 without prejudice or disclaimer.

Remarks

Claims 1-8, 10 and 12-22 remain pending in the application. Claims 9 and 11 have been deleted without prejudice. Claim 1 has been amended to more clearly define the subject matter claimed. A marked-up copy of claim 1 indicating the amendment is attached hereto as Appendix A.

The Examiner has rejected all pending claims under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,345,300 issued to Bakshi *et al.* (hereinafter "Bakshi"). Applicants respectfully traverse this rejection for the following reasons.

While Applicants address the rejected claims below, Applicants would like to first provide the following overview of Applicants' technology that the Examiner may find helpful. A host computer is used to distribute, store and retrieve electronic information associated with a particular end user. The host computer assembles the information associated with the particular end user and transmits this information to a client computer associated with the particular end user.

When the end user wishes to access the assembled information, she initiates a request to the host computer using a software package, such as a Web browser; the client computer will typically run this software package. The host computer receives the request concerning the information. The host computer receives the previously transmitted information from the client computer either as part of the transmitted request or as a separate transmission. The host computer proceeds to service the request to generate a request result, which is then forwarded to either the software package initiating the request or another specified delivery platform.

Bakshi relates to systems and methods for detecting a user-controlled parameter from a client device residing behind a proxy. The Bakshi systems and methods enable a network device, such as one capable of providing customized transcoding services, to acquire user-specified preferences from a client device which accesses that network device through a firewall or other proxy. Bakshi, 2:2-10. The purpose of systems and methods disclosed in Bakshi is to solve the inability to obtain user specific information when servicing a request from a client device to an external network resource through a firewall or other network proxy. Bakshi, 1:49-67.

Claim 1 stands rejected as anticipated by Bakshi for the reasons stated in paragraph 4 of the Office Action. First, the Examiner asserts that Bakshi discloses aggregation of data associated with the end user by the host computer from one or more information providers. The Examiner cites the description of the server-side cache disclosed in Bakshi for this assertion. The server-side cache in Bakshi, however, does not aggregate data associated with the end user; rather, the server-side cache stores "both original and transcoded versions of content for later transmission to the network client 12 without the need to re-retrieve the content from the Internet 18 or to re-transcode the content." Bakshi, 4:2-5. First, under the claimed method, the aggregated data is accumulated from one or more information providers. This aggregated data is associated with a particular end user. The server-side cache simply stores previously requested network objects in original and/or transcoded format. These network objects need not have any association with any particular end user, or network client. Further, the aggregated data associated with end user according to claimed method need never be stored on the host computer. According to claim 1 as amended, the aggregated data is transmitted to the client computer, thereby causing the client computer to store the aggregated data. Applicants assert that the storage of unassociated, previously retrieved network objects in one or more formats as seen in Bakshi does not teach or suggest the aggregation by a host computer of data

associated with a particular end user from one or more information providers that is transmitted to a client computer for storage.

Further, the Examiner asserts that Bakshi discloses the limitation of receipt of aggregated data associated with the end user by the host computer. The Examiner supports this contention by citation to the description of Bakshi's acquisition of user preferences by a network proxy. In Bakshi, however, the network proxy must then acquire the requested network object either from a local server-side cache or a content server. In contrast, the method of claim 1 services the received request using the aggregated data received from the client computer; the host computer, therefore, is not required to acquire content from either a local server-side cache or a content server. One benefit of the claimed method is that the data for servicing the request is stored on the client computer itself rather than on the host computer. Accordingly, if the security of the host computer is compromised, the aggregated data is not available to the intruder.

For at least the reasons above, Applicants believe that claim 1 as amended is allowable over Bakshi. Independent claims 17 and 25 both include analogous limitations to those detailed above with respect to claim 1, and therefore, should be allowable over Bakshi for the same reasons as cited with respect to claim 1. As claims 2-8, 10 and 12-16 depend directly or indirectly from claim 1 and as claims 18-24 depend directly or indirectly from claim 17, these dependent claims also include the limitations discussed above with respect to claim 1, and therefore, should similarly be allowable. Applicants respectfully request that the Examiner withdraw the rejection of these claims.

In additions, claims 4 and 17 introduce a limitation that the aggregated data be encrypted prior to transmission to the client computer. Claims 5-7 and 18-19 depend directly or indirectly from claims 4 and 17 respectively; consequently, these claims also include this encryption limitation. The Examiner cites Bakshi's transcoding services as anticipating this limitation. Applicants respectfully assert that the transcoding services as described in the cited portions of Bakshi only identify compression and scaling as

transcoding services. These cited portions do not teach the encryption of data transmitted to the client. In fact, Bakshi's transcoding services are aimed at altering content received by the transcoding server in order to deliver the content in a format more usable by the client device. By requiring encryption of the aggregated data prior to transmission in these claims, the content aggregated by the host computer from the one or more information providers is modified to make it harder for the client computer to use rather than easier. By encrypting the aggregated data prior to transmission thereby causing the client to store the encrypted aggregated data, an additional layer of security is introduced. If the host computer's integrity is compromised, the aggregated data is not available to the intruder since it has been sent to the client computer. If the client computer is compromised, the aggregated data is stored in an encrypted form.

For at least these additional reasons, Applicants believe that claims 4-7 and 17-19 are patentable over Bakshi. Bakshi does not teach the encryption of aggregated data associated with a particular end user prior to transmission of the aggregated data to a client computer associated with the end user. Applicants respectfully request that the Examiner withdraw the rejection of these claims.

Conclusion

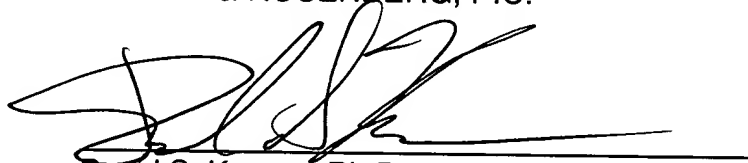
For at least the reasons stated above, the Applicants respectfully submit that each of the claims pending in the application is allowable, and therefore courteously solicit the allowance of the claims.

The Examiner is invited and encouraged to directly contact the undersigned if such contact may enhance the efficient prosecution of this application to issue.

No additional fee is believed to be due with this response. If, however, the Commissioner believes that a fee is due, the Commissioner is hereby authorized to charge any such additional fee(s) from, or credit any fee overpayment(s) to, Deposit Account No. 14-0629.

Respectfully submitted,

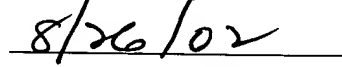
NEEDLE & ROSENBERG, P.C.


David S. Kerven, Ph.D.
Registration No. 43,712

Certificate of Mailing

I hereby certify that this correspondence and any items indicated as attached or included are being deposited with the United States Postal Service in an envelope addressed to: BOX NON FEE AMENDMENT, Commissioner for Patents, Washington, D.C. 20231, on the date indicated below.


Lucy J. Lehman


Date

APPENDIX A
MARKED UP COPY OF THE CLAIM

1. (Amended) A method for distributing, storing and retrieving data associated with an end user aggregated from one or more information providers between a host computer and a client computer associated with the end user, comprising the steps of:
- (a) aggregating data associated with the end user by the host computer from one or more information providers;
 - (b) transmitting the aggregated data from the host computer to the client computer, thereby causing the client computer to store the aggregated data;
 - [(c) receiving at the client computer the aggregated data from the host computer;
 - (d) storing the received aggregated data at the client computer;]
 - [(e)c] receiving by the host computer a request concerning the aggregated data;
 - [(f)d] receiving by the host computer the stored aggregated data from the client computer; and
 - [(g)e] servicing by the host computer the received request based on the received, stored aggregated data to generate a request result.